

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

In re Application of KARAM SALAH)
AL DIN AWNI AL SADEQ and)
STOKOE PARTNERSHIP SOLICITORS)
for an Order Under) 1:21mc6
28 U.S.C. § 1782 to Conduct)
Discovery for Use in Foreign)
Proceedings.)

MEMORANDUM OPINION AND ORDER

This case comes before the Court on the “*Ex Parte* Application for an Order Under 28 U.S.C. § 1782 to Conduct Discovery for Use in Foreign Proceedings” (Docket Entry 1) (the “Application”).¹ For the reasons that follow, the Court will grant the Application.²

1 For legibility reasons, this Memorandum Opinion uses standardized capitalization, but retains the British spelling and punctuation in all quotations.

2 “Courts disagree over whether a Section 1782 proceeding, or a motion thereunder, is a dispositive motion requiring the magistrate judge to issue a report and recommendation.” In re Peruvian Sporting Goods S.A.C., No. 18-mc-91220, 2018 WL 7047645, at *3 (D. Mass. Dec. 7, 2018) (collecting cases). However, the United States Court of Appeals for the Fourth Circuit has affirmed, under an abuse of discretion standard, a district court judge’s affirmation, under the clearly erroneous or contrary to law standard, of a magistrate judge’s grant of a Section 1782 application. See generally In re Naranjo, 768 F.3d 332 (4th Cir. 2014) (explaining that, in ruling on Section 1782 application, “the magistrate judge ordered [certain individuals] to turn over the documents that they possessed” and, “[o]ver objection, the district court affirmed the magistrate judge’s decision in a July 16, 2013 order,” id. at 341-42; analyzing substantive challenges to magistrate judge’s rulings, see id. at 347-51; and “affirm[ing] the district court’s order in the § 1782 proceeding,” id. at 351, under “the familiar abuse-of-discretion standard,” id. at 347); see also Chevron Corp. v. Page, No. 8:11cv395, Docket Entry 74 at 1 (D. Md. July 16, 2013) (overruling objections to magistrate judge’s Section 1782 order, “the Court concluding that the challenged Order was neither clearly erroneous nor contrary to law”), affirmed In re (continued...)

BACKGROUND

Karam Salah Al Din Awni Al Sadeq ("Al Sadeq") and Stokoe Partnership Solicitors ("Stokoe," and collectively, the "Applicants") have moved, "pursuant to 28 U.S.C. § 1782 and Federal Rules of Civil Procedure 26 and 45" (Docket Entry 1 at 1), for leave to serve two subpoenas on Nicholas Del Rosso ("Del Rosso") (Docket Entry 3-1 at 2) and "Vital Management Services Inc." ("Vital Management") (Docket Entry 3-2 at 2) in connection with ongoing litigation in the United Kingdom (at times, the "UK"). (See Docket Entry 1 at 1-2, 4-6.)³ They further "request[ed] that the Court grant such leave *ex parte*." (Id. at 1.) In support of their request, Applicants provided the "Declaration of Haralambos Tsiattalou" (Docket Entry 4) (the "Tsiattalou Declaration"), with various attachments (see Docket Entries 4-1 to 4-15), the "Declaration of Mark W. Merritt" (Docket Entry 3) (the "Merritt

2 (...continued)
Naranjo, 768 F.3d at 351; 28 U.S.C. § 636(b)(1) (applying "clearly erroneous or contrary to law" standard to magistrate judge orders on "any pretrial matter" not specifically exempted under Section 636(b)(1)(A), and applying de novo standard to magistrate judge recommendations on eight "motion[s] excepted in subparagraph (A)," none of which involve Section 1782 applications). Accordingly, the undersigned United States Magistrate Judge will issue an order rather than a recommendation on the Application.

3 Applicants assert that, "[u]pon information and belief, Del Rosso is the owner and president of Vital Management." (Docket Entry 2 at 4 n.2; see also Docket Entry 4-4, ¶ 1 (Del Rosso witness statement characterizing Del Rosso as "President and owner of Vital Management").)

Declaration"), and the proposed subpoenas (see Docket Entries 3-1, 3-2).

I. Factual Background

According to Applicants:

Haralambos Tsiattalou ("Tsiattalou"), "a partner at [Stokoe, a] UK-based law firm," serves as Al Sadeq's lawyer "in civil proceedings pending in the High Court of Justice of England and Wales, Queen's Bench Division captioned *Karam Salah Al Din Awni Al Sadeq v. Dechert, LLP, Neil Gerrard, David Hughes, and Caroline Black*, Claim No. QB-2020-000322 (the 'Al Sadeq Litigation[')']." (Docket Entry 4, ¶ 1.) In turn, Stokoe "is the Claimant in civil proceedings pending in the High Court of Justice of England and Wales, Queen's Bench Division captioned: *Stokoe Partnership Solicitors v. Mr. Patrick Tristram Finucane Grayson, Grayson + Co Limited, Mr. Stuart Robert Page, and Page Corporate Investigations Limited*, Claim No.[] QB-2020-002492 (the 'Grayson Proceeding[,]' and collectively with the Al Sadeq Litigation, the "Foreign Proceedings"). (Id.) "Stokoe was also the claimant in concluded High Court proceedings captioned: *Stokoe Partnership Solicitors v. Mr. Paul Robinson, Company Documents Limited, and Mr. Oliver Moon*, Claim No. QB-2020-002218 (the 'Robinson Proceeding[,]' and collectively] with the Grayson Proceeding[,]. . . the 'Hacking Claims')." (Id.)

The Al Sadeq Litigation concerns alleged violations of international and United Arab Emirates (the "UAE") law, as well as of Al Sadeq's human rights, committed "by Neil Gerrard ('Gerrard'), a solicitor and partner in Dechert UK [('Dechert')], and [two other current or former Dechert partners, David Hughes ('Hughes') and Caroline Black ('Black')] (collectively with Dechert and Gerrard, the 'Dechert Defendants'),] in connection with their investigation of fraud allegedly perpetrated against the RAK Investment Authority ([the] 'RAKIA')" (id., ¶ 4). (See id., ¶ 2, 4.)⁴ Al Sadeq denies involvement in the alleged fraud and "maintains that the charges against him were politically motivated . . . and that he was convicted on the basis of false confessions obtained from him under duress by [Dechert] Defendants." (Docket Entry 4-1, ¶ 1.)

Al Sadeq served as legal adviser, Group Legal Director, and, ultimately, Deputy Chief Executive Officer of RAKIA between 2008 and 2012. (Id., ¶ 35.) In this capacity, he worked with Dr. Khater Massaad ("Dr. Massaad") (see id.), RAKIA's former Chief Executive Officer (the "CEO") (see id., ¶ 8), and also "had regular interactions with," and was well known to (id., ¶ 36), Sheikh Saud Bin Saqr Al-Qasimi, who, beginning in 2003, held the title of "Crown Prince and Deputy Ruler of RAK" (id., ¶ 12; see also id., ¶ 19 (discussing timing of that appointment)), before, "in October

⁴ "RAK" signifies Ras Al Khaimah, "one of the constituent Emirates of the UAE" (Docket Entry 2 at 5). (See id. at 6.)

2010, . . . succeed[ing] his father as Emir of RAK" (id., ¶ 22).⁵ From at least 2003 until 2010, "Dr Massaad was the Ruler's close friend and confidant, in his presence on a daily, or almost daily, basis." (Id., ¶ 12.)

In 2005, "RAKIA was established" (id., ¶ 14), and, from that time until approximately 2012, Dr. Massaad served as RAKIA's CEO, controlling the "day to day management of RAKIA" and "developing investment strategies and taking investment decisions with the knowledge, approval, and instructions of the Ruler" (id., ¶ 15). "[B]y around 2010 RAKIA had, with the full knowledge and approval of the Ruler, very significant investment interests outside RAK, particularly in Georgia" (Id., ¶ 17.) For various political, familial, and economic reasons beginning around 2008, the Ruler directed that RAKIA should "divest itself of its foreign investments" (id., ¶ 21), a sudden change in investment policy that adversely affected the return on certain RAKIA investments (see id.), after which a rift developed between the Ruler and Dr. Massaad. (See id., ¶¶ 15-25.)

Dr. Massaad "left RAK in around June 2012, on good terms and without any suggestion of wrongdoing," and "returned to the UAE on several occasions thereafter until August 2014, including for meetings with the Ruler." (Id., ¶ 25.) However, in approximately

⁵ Despite the change in title during the relevant period, for ease of reference, this Memorandum Opinion refers to the above-referenced individual as "the Ruler."

2014, the Ruler learned that one of his brothers, Sheikh Faisal, whom the Ruler had denied appointment as Crown Prince following the Ruler's succession in October 2010 (id., ¶ 23), "causing animosity between them" (id., ¶ 26), served as an investor in a business that Dr. Massaad founded in Lebanon in 2012. (See id., ¶¶ 26-27.) "As a result, the Ruler became concerned that Dr Massaad was working with Sheikh Faisal and / or Sheikh Khaled^[6] in order to destabilise the Ruler, and that Sheikh Faisal and / or Sheikh Khaled were plotting to remove the Ruler with the assistance of Abu Dhabi" (id., ¶ 27), "the most powerful of the Emirates" (id., ¶ 20).

In particular:

Since finding out about Dr Massaad's business relationship with Sheikh Faisal in 2014 and following on from the fall-out between Dr Massaad and the Ruler, and the Ruler's concerns about Dr Massaad's involvement in suspected moves to oust him by Sheikh Khaled and Sheikh Faisal, the Ruler with the assistance of [Dechert] Defendants has pursued a vendetta against Dr Massaad and alleged co-conspirators such as . . . [Gela] Mikadze[(at times, "Mikadze")^{7]} and [Farhad] Azima [("Azima")^{8]}

6 "Sheikh Khaled was the Crown Prince and Deputy Ruler [of RAK] between around 1958 until around June 2003 when the [Ruler's father] removed [Sheikh Khaled] and replaced him with the Ruler. This was an unpopular move in some quarters leading to street protests in favour of Sheikh Khaled in RAK, and he retained significant support in the Emirate to succeed the [Ruler's father]." (Id., ¶ 19.)

7 Mikadze formerly served as "General Manager of RAKIA's Georgia operations." (Id., ¶ 9.5.)

8 "[A] US-Iranian businessman," Azima "had dealings with RAKIA" (id., ¶ 9.5) and has engaged in litigation with RAKIA in the UK courts (see id., ¶ 62).

(including by recent proceedings in the English High Court [(the "Azima Litigation")⁹]).

The background set out above . . . is the context in which wrongs have been committed against [Al Sadeq] who has become collateral damage in the vendetta pursued by the Ruler against Dr Massaad, against whom RAKIA allegedly seeks to recover over USD 2 billion. The Ruler's motive in pursuing his vendetta is both to punish Dr Massaad for his supposed disloyalty by destroying his reputation and discrediting him, and also to attempt to conceal the Ruler's own personal knowledge and direction of RAKIA's foreign investments for his own personal and political benefit in the years before his accession. In this regard, it is a matter of public record that Mr Gerrard was appointed by the Ruler in order to investigate and pursue Dr Massaad; and Mr Al Sadeq and his wife were told both by Mr Gerrard and Mr Hughes that the "Big Bastard" Dr Massaad, and his alleged co-conspirators, were the people they were really after, and that they merely wanted Mr Al Sadeq's "cooperation" to help them build that case. Despite several criminal sentences having been pronounced against Dr Massaad by the RAK courts in absentia, Dr Massaad maintains his innocence and presently lives and works in Saudi Arabia, an Interpol notice which had been lodged against him by RAK now having been removed, and an extradition request from RAK having been dismissed by the Saudi court.

(Id., ¶¶ 28-29 (internal paragraph numbering omitted).)

"RAK is regarded by international observers as having a record of human rights abuses including arbitrary detention, forced

9 In the Azima Litigation, RAKIA sued Azima for alleged fraudulent misrepresentation, conspiracy, and breach of warranty (see, e.g., Docket Entry 4-2, ¶¶ 5-10), relating in part to an allegedly sham referral agreement connected to the sale of a Georgian hotel, the creation of which involved Al Sadeq (see, e.g., id., ¶¶ 168-181.6). In response, Azima "contend[ed] that the claims should be struck out or dismissed on the ground that, in bringing the claims, RAKIA [wa]s relying on confidential emails that RAKIA obtained through its unlawful hacking of his email accounts." (Id., ¶ 10.) Azima also "counterclaim[ed] for damages resulting from what he allege[d] was RAKIA's hacking of his emails." (Id.)

confessions, unfair trials, and mistreatment in detention.” (Id., ¶ 30.) Per the “Particulars of Claim” in the Al Sadeq Litigation (id. at 2) (at times, the “Al Sadeq Claim”):

Al Sadeq’s treatment follows a similar pattern to the examples [of human rights violations specified in a 2014 Amnesty International report detailed in the Al Sadeq Claim] in that, *inter alia*, he was kidnapped, arbitrarily detained for over five years, subjected to torture and inhumane treatment while incarcerated in solitary confinement for around 560 days, denied access to legal representation, only occasionally allowed to see his family, his family was denied information about his whereabouts at all material times until April 2016, his family was threatened and he was forced to sign false confessions under duress which were used in order to convict him and to implicate others including Dr Massaad. [Dechert] Defendants were aware of the abuse to which Mr Al Sadeq was subjected, which [as] pleaded [in the Al Sadeq Claim] was orchestrated by Mr Gerrard with the assistance of the other [Dechert] Defendants, at the behest of the Ruler.

(Id., ¶ 33.)

“In summary,” according to the Tsiattalou Declaration, the Al Sadeq Claim alleges Dechert Defendants’ involvement in:

- a. The kidnap and extraordinary rendition of Mr. Al Sadeq from Dubai to RAK (see paragraphs 40 to 47 of the Al Sadeq Claim);
- b. Mr. Al Sadeq’s unlawful detention without arrest or charge, including a period of detention in solitary confinement, under a false name, with no access to legal representation (see paragraphs 105 to 109 of the Al Sadeq Claim);
- c. The interrogation of Mr. Al Sadeq. In particular, Mr. Al Sadeq contends that during the first of his interrogations by Mr. Gerrard, he was blindfolded with his hands tied behind his back and had no lawyer present (see paragraph 64 of the Al Sadeq Claim);

d. Threats and unlawful pressure made to Mr. Al Sadeq, his wife, and children, including a promise by Mr. Gerrard and Ms. Black that Mr. Al Sadeq's prison conditions could be improved if he "cooperated" with them (see paragraphs 65 to 67, 89 to 98, and 120 to 130 of the Al Sadeq Claim);

and

e. The procurement of false confessions signed by Mr. Al Sadeq, but drafted by Mr. Gerrard and Mr. Hughes, in circumstances where Mr. Al Sadeq was detained in the above conditions, did not have access to legal representation, and had made it clear that the confessions were untrue (see paragraphs 183 to 184 of the Al Sadeq Claim).

(Docket Entry 4, ¶ 5.)

Given the "extremely serious nature" of Al Sadeq's allegations "against senior lawyers and a global law firm of international repute[,]. . . . the Al Sadeq Litigation has generated a significant degree of publicity in the UK." (Id., ¶ 6.)

"Stokoe was first retained to act in the Al Sadeq Litigation in October 2019. Since that time, there has been a correlation between the progress of the Al Sadeq Litigation and attempts to obtain confidential information from Stokoe and others in relation to those proceedings." (Id., ¶ 7.) On January 28, 2020, "[t]he Claim Form in the Al Sadeq Litigation was issued" and, although Stokoe did not serve it at that time, its "allegations were made public in a press release published by Detained in Dubai on the date of issue." (Id., ¶ 8.)¹⁰ "The Claim Form, which was made

10 An employee of "the London-based human rights advocacy (continued...)

available online, was much more detailed than the amended version ultimately served with the Particulars of Claim and contained details of Mr. Al Sadeq's claim and the nature of the allegations made against the Al Sadeq Litigation defendants." (Id.)¹¹ The Claim Form also disclosed that "Stokoe was acting on behalf of Mr. Al Sadeq." (Id.)

In February and March 2020, Tsiattalou and other members of "Al Sadeq's Legal and Support Team" (id., ¶ 3)¹² traveled to Dubai to meet with Al Sadeq's local counsel and Al Sadeq, although they ultimately did not receive permission to visit Al Sadeq (who remained incarcerated in the RAK Central Prison as of March 31, 2020 (see Docket Entry 4-1, ¶ 214; see also id. at 65)). (Docket Entry 4, ¶ 10.) During these trips, Tsiattalou and other members of Al Sadeq's Legal and Support Team

were the subject of surveillance activities, including an apparent break-in to [Tsiattalou's] hotel room, the presence of surveillance agents at [Tsiattalou's] hotel (where [Tsiattalou] attended privileged meetings in relation to the conduct of the Al Sadeq Litigation), and

10 (...continued)
organization 'Detained in Dubai,'" Radha Stirling, has assisted Al Sadeq. (Id., ¶ 14.)

11 "Al Sadeq's Amended Claim Form and Particulars of Claim were served on March 31, 2020 and April 1, 2020." (Id., ¶ 9.) The Amended Claim Form details "various ways" that Stokoe's "ability to take instructions from Mr. Al Sadeq has been impeded . . . since the Al Sadeq Litigation was issued." (Id.)

12 Stokoe, 4 Stone Buildings (another UK law firm), Detained in Dubai, and Maltin Litigation Support Group collectively comprise "Al Sadeq's Legal and Support Team." (Id.)

an attempt to follow [Tsiattalou] to a privileged meeting at a different location. [Tsiattalou] believe[s] these matters were also connected to the Al Sadeq [L]itigation and that they were intended to disrupt [his] ability to obtain instructions (as they in fact did).

(Id.; see also Docket Entry 4-1, ¶¶ 215-215.10 (detailing surveillance and interference allegations).) During a visit in March 2020, Tsiattalou and his colleagues “were subject to intimidation and surveillance” and “an obviously frightened hotel employee” warned Tsiattalou:

“You’re being followed/watched by security services. They are very serious people. Nobody can stand in their way.”

(Docket Entry 4, ¶ 11.) Tsiattalou believes that Mr. Stuart Page (at times, “Page”), who Tsiattalou “personally witnessed” on March 6, 2020, “whilst staying at the One and Only on the Palm Hotel in Dubai” (id., ¶ 21), and who admitted his presence at Tsiattalou’s Dubai hotel on that date, conducted this surveillance, along with other individuals. (Id., ¶ 12.)

According to the opinion of Judge Lenon, “sitting as a Deputy Judge of the Chancery Division” (Docket Entry 4-2 (the “Azima Judgment”) at 2 (emphasis omitted)), issued in the Azima Litigation, “[i]n January 2015 Stuart Page, a private investigator, was engaged by the Ruler to investigate what the Ruler feared was

a plot between a member of his family and Dr Massaad aimed at destabilising his rulership." (Id., ¶ 31.)¹³

The Azima Judgment further explained:

In March 2015 Mr Page provided the Ruler with a report entitled RAK Project Update ("the Project Update") which was mainly concerned with Dr Massaad's activities but which also described how Mr Azima was managing a team of advisers in the US, hired by Dr Massaad, who were planning to spread allegations about human rights issues in RAK;^[14] their campaign had not yet been made public. Mr Page's agents who compiled the report said that they would be able to gather intelligence on the campaign team

13 "Mr Page's initial engagement in RAK was between 2008 and 2010 when he undertook surveillance work on the behalf of the Ruler who was at the time the Crown Prince. His remit was to try to ascertain through surveillance what plans Sheikh Khalid, the Ruler's brother, had to try to destabilise the Crown Prince's position." (Id., ¶ 260.)

14 These stories involved the alleged mistreatment of Al Sadeq and his wife, including the involvement of Dechert and/or Gerrard in Al Sadeq's interrogations and detention. (See, e.g., Docket Entry 4-2, ¶¶ 197-201.8.) According to Judge Lenon:

In order to make good its case that Mr Azima procured and promoted false stories in the media, it was incumbent on RAKIA to establish that the stories which it was intended to publish about human rights violations were untrue. It has not done so. It appears that Project Clay[, which RAKIA described as "a coordinated programme designed to frustrate RAKIA's attempts to pursue legal remedies against Dr Massaad by procuring and promoting the widespread publication of damaging false stories in the international media" (id., ¶ 198.1),] intended to draw attention to actual cases of detention and illegality, not fabricated cases. The 2014 Amnesty International Report indicates that there were real grounds for concern about detention procedures in RAK. None of RAKIA's witnesses were in a position to refute the findings in that report.

(Id., ¶ 202.)

in order to monitor their progress and "attempt to contain or ruin their plans".

Neil Gerrard is a former policeman and a partner in the firm of Dechert LLP which was instructed to assist with the investigation into Dr Massaad's alleged fraudulent activities which it has continued to work on to the present time. His witness statement dealt with his engagement by RAK, the meeting he had with Mr Azima in July 2016 and the events in August 2016 surrounding the downloading of [Azima's] hacked material. He was cross-examined about his involvement with the questioning of detainees within RAK, in particular Karam Al Sadeq and Shahab Izadpanah. Allegations that Mr Gerrard had attempted, on behalf of RAK, to extort money from Mr Izadpanah and had offered Mr Izadpanah and Mr Al Sadeq to drop all charges against them if they confessed to charges implicating Dr Massaad were put to Mr Gerrard who denied them in forthright terms. On the basis of the material before [Judge Lenon, he was] not in a position to make any findings in relation to those allegations or other allegations of misconduct extraneous to the events in issue in these proceedings that were put to Mr Gerrard.^[15]

15 Following entry of the Azima Judgement, and prompted by the Al Sadeq Litigation, Gerrard disclosed that he provided false testimony in the Azima Litigation regarding the nature and extent of his interactions with Al Sadeq and his wife. See generally Azima, Docket Entry 22-2. As relevant here, Judge Lenon "agree[d] with Mr Azima's submission that the corrected evidence cumulatively creates a materially different impression of the extent and nature of Mr Gerrard's dealings with Mr Al Sadeq." Id., Docket Entry 22-2, ¶ 14. Judge Lenon further rejected "RAKIA's submission that the erroneous evidence goes to peripheral matters which were of no relevance to the substantive issues. There was a pleaded issue on RAKIA's own case in the proceedings as to whether the stories about human rights abuses and Dechert's involvement in those abuses were false" Id., Docket Entry 22-2, ¶ 15 (citing Docket Entry 4-2, ¶¶ 197-198). However, Judge Lenon declined to reopen the Azima Judgment because, inter alia, he found that disclosure of Gerrard's false testimony and his subsequent revisions thereto did not alter "[Judge Lenon's] conclusions on any of the substantive issues." Id., Docket Entry 22-2, ¶ 22.

Counsel for Mr Azima submitted that Mr Gerrard gave dishonest evidence on key issues. He was also criticised for not referring to Mr Page and the Project Update in his witness statement. In [Judge Lenon's] view, Mr Gerrard's witness statement should have dealt with the Project Update which was a clearly relevant document and one which, as he accepted in cross-examination, was of concern to him when it was produced because it referred to the threat of a press campaign to smear RAK and its Ruler with human rights allegations. [Judge Lenon] do[es] not, however, regard the omission to deal with the Project Update, or the other criticisms made of his evidence, as leading to the conclusion that [Judge Lenon] should treat Mr Gerrard as dishonest.

Stuart Page, also a former policeman and now the Chairman and majority shareholder of a business providing security and surveillance services, dealt in his witness statement with his engagement in RAK to assist with the investigations into Dr Massaad and the discovery of the hacked material. Counsel for Mr Azima submitted that Mr Page was a dishonest witness who lied about a number of matters. [Judge Lenon] consider[s] that Mr Page was an unsatisfactory and unreliable witness. As set out in greater detail in the context of the [Azima] hacking claim, his witness statement was misleading in relation to two significant matters. First, his witness statement implied that he did not produce written reports for the Ruler on his investigations whereas in fact he did so on a regular basis. Second, his witness statement said that he first came across the name of Mr Azima in early 2016 whereas . . . it was in fact a year earlier. His evidence in connection with the discovery of the hacked material was both internally inconsistent and at odds with the contemporary documents. [Judge Lenon] ha[s] concluded that it would be unsafe to rely on any evidence from Mr Page that was not corroborated by some other source.

[Three referenced cases involving Page and illegally obtained information] highlight the fact that Mr Page operates in a world of covert surveillance in which agents acquire confidential information unlawfully and that Mr Page has dealings with such agents. It would be a reasonable inference to draw from these incidents that Mr Page has access to agents with the capacity to hack

emails. However these other incidents do not establish that Mr Page ever personally carried out or authorised the unlawful obtaining of confidential information and therefore do not affect [Judge Lenon's] assessment of the inherent likelihood of Mr Page acting unlawfully in this case. Mr Azima also relied on the level of Mr Page's remuneration of between \$100,000 and \$300,000 per month as being "consistent with Mr Page obtaining information by illicit means and of seeking a premium for such nefarious activity." Mr Page was certainly generously remunerated but [Judge Lenon] do[es] not consider that his rate of remuneration can sensibly be taken as a sign of illicit activity.

(Id., ¶¶ 32, 62-64, 369 (internal paragraph numbering omitted).)

In the Azima Litigation, RAKIA maintained that Page innocently discovered websites containing Azima's hacked emails, which Gerrard then enlisted Del Rosso to download, a task Del Rosso achieved with the help of Northern Technology Inc. ("NTi"). (See, e.g., id., ¶¶ 51-53, 336-343.11.)¹⁶ Judge Lenon "conclude[d] from the unexplained contradictions, inconsistencies and implausible elements that RAKIA's case that Mr Page discovered the blogging websites linked to the BitTorrent sites [containing Azima's hacked data] innocently via [an Israeli journalist] and another unidentified informer is not true and that the true facts as to how RAKIA came

¹⁶ In support of this contention, RAKIA submitted a witness statement from Del Rosso that attributes the discovery of all but one batch of data to Page and the discovery of the final data batch to an NTi employee. (See generally Docket Entry 4-4.) Del Rosso's witness statement further indicates that, in August 2014, Dechert engaged Vital Management "to investigate assets potentially stolen from the Government of [RAK]. Pursuant to its engagement[, Vital Management] examined potential frauds committed by, amongst others, [Dr.] Massaad." (Id., ¶ 4.) Del Rosso "took [his] instructions from Dechert LLP, and had limited direct contact with Jamie Buchanan and other representatives of the RAK government." (Id.)

to know about the hacked material have not been disclosed.” (Id., ¶ 355; see also id., ¶¶ 342-54 (examining evidence and assertions).) Per Judge Lenon, though, “[i]t does not of course necessarily follow from this conclusion that RAKIA was responsible for the hacking.” (Id., ¶ 356.)

As to Azima’s hacking claim, Judge Lenon ultimately

accept[ed] that the hypothesis advanced on behalf of Mr Azima that Mr Page, acting with the express or implied authority of the Ruler, arranged for Mr Azima’s emails to be hacked . . . and that it was decided to deploy the hacked material in August 2016 once [a] ceasefire with Dr Massaad was over, is not impossible. It would provide an explanation for the fact that the hacked material came to light when it did and for RAKIA’s failure to provide a convincing account of its innocent discovery of the hacked material. It is equally not impossible that Mr Page arranged for Mr Azima’s emails to be hacked without the knowledge of Mr Gerrard or [James] Buchanan [(“Buchanan”)¹⁷] or the Ruler’s advisers so that the instigation of these proceedings did not entail a conspiracy between them, even though the witnesses may have harboured suspicions about Mr Page’s role.

17 Buchanan served as a representative of RAK and the CEO of Ras Al Khaimah Development LLC (see, e.g., Docket Entry 4-1, ¶ 143; Docket Entry 4-4, ¶ 4), an entity “which holds and manages assets and liability previously owned by [RAKIA], and is thus intimately tied to the Al Sadeq Litigation” (Docket Entry 6, ¶ 15). Per the Azima Judgment:

In around April 2015, the Ruler told Mr Buchanan that he wanted Mr Buchanan and other assistants to “target” Mr Azima. The Ruler directed his associates to bring charges against Mr Azima. The Ruler’s associates discussed meeting to “coordinate our attack” on Mr Azima and Dr Massaad but persuaded the Ruler not to pursue this plan at that time.

(Docket Entry 4-2, ¶ 33.)

It is, however, not enough for Mr Azima to advance a case that is not impossible. Based on all of the documentary and witness evidence, [Judge Lenon] was not satisfied on the balance of probabilities that RAKIA was responsible for the hacking of Mr Azima's emails. The facts supporting the inference that RAKIA was responsible for the hacking are far from conclusive and the improbable features of Mr Azima's case can only be explained away on the basis of speculative assumptions for which there is no sufficiently firm evidence.

(Id., ¶¶ 380-381 (internal paragraph numbering omitted).)

Accordingly, Judge Lenon denied Azima's hacking counterclaim.

(See id., ¶¶ 382-84.)

On appeal, Azima sought to introduce new evidence relevant to his hacking claims. As the UK appellate court explained:

A tip-off from Thomson Reuters after the trial led Mr Azima to conclude that he had not been the only victim of spear-phishing^[18] emails but that others who had been named in the Project Update had also been targets. Linked with the tip-off was a report by The Citizen Lab released on 9 June 2020 which claimed to have uncovered a "massive hack-for-hire operation" said to be linked to an Indian company called BellTrox.

The information provided by Thomson Reuters consisted of email addresses (both recipients and senders) together with dates and times of sending, beginning in March 2015. The recipients included not only Mr Azima but also others who had been named in the Project Update. Following the information provided by Thomson Reuters Mr Azima's computer expert (who had given evidence at trial) produced a further report in which he

18 Tsiattalou explained that phishing and spear-phishing communications "seek to trick the recipient into clicking on a link to a website which itself contains malicious software which is downloaded onto the recipient's device. Spear-phishing is a more sophisticated form of phishing where the communication contains specific information, targeted at the recipient, which makes it more likely that the recipient will click on the link." (Docket Entry 4, ¶ 43.)

said that certain features of the material demonstrated that these emails were spear-phishing emails. This evidence was said to show that Mr Azima had been the target of phishing emails which began at the same time as the Project Update was provided to RAKIA: that is to say in March 2015. RAKIA's computer expert (who had also given evidence at trial) made a number of sustained criticisms of that report. RAKIA also took the point that since one of the allegations at trial was that Mr Azima's emails had been hacked because he was named in the Project Update, it would have been open to him to have asked the others also named in that report to allow access to their email accounts. Indeed, RAKIA had applied for disclosure from at least three of those individuals, which Mr Azima refused.

Mr Azima subsequently instructed Mr Rey, a security consultant based in Switzerland, to investigate. Mr Rey's investigations into BellTrox led him to another Indian company called CyberRoot. He spoke to a Mr Vikash Kumar Pandey, a former employee of CyberRoot. Mr Pandey told him that he and four of his colleagues had worked on the hack of Mr Azima on the instructions of Mr Del Rosso (who had given evidence for RAKIA at trial,^[19] but had not mentioned CyberRoot). Mr Pandey began working on the hack in June or July 2015; that is to say some three to four months after the date of the Project Update. Mr Pandey described the methods that he and his colleagues had used. CyberRoot's efforts to hack Mr Azima's emails were initially unsuccessful; but they gained access to them in March 2016. He also described how CyberRoot had disseminated Mr Azima's information on the internet. CyberRoot had been paid about \$1 million for this work.

In response to this evidence Mr Del Rosso made another witness statement. He accepted that he had engaged CyberRoot to carry out work on RAKIA's behalf; and had arranged the payment to CyberRoot of the \$1 million. But he said that that was for different work which had nothing to do with Mr Azima.

19 In his witness statement in the Azima Litigation trial, Del Rosso maintained that he "did not hack Mr Azima's computers, cause him to be hacked or know who hacked him. [Del Rosso] did not upload his data to the internet, cause his data to be uploaded or know who did upload his data." (Docket Entry 4-4, ¶ 20.)

Whether RAKIA was involved in the hacking is hotly in dispute. Moreover, Mr Panday's account of how the hacking began is at variance both with Mr Azima's case and also with what the first tranche of fresh evidence is said to demonstrate. His evidence is that CyberRoot only gained access to Mr Azima's email accounts in March 2016, whereas Mr Azima's case was that the hacking had taken place many months earlier. If RAKIA had already obtained access to Mr Azima's email accounts many months earlier, it is difficult to see why CyberRoot would have been instructed to replicate the hacking. Nevertheless, if Mr Panday's account is true, it seems to [the appellate court] that it will support Mr Azima's allegation that RAKIA was responsible for the hacking (although not the way in which it was put at trial); and that RAKIA's defence to the counterclaim was dishonestly advanced. That will in [the appellate court's] judgment require a complete re-evaluation of the evidence in support of the hacking claim.

Azima v. Del Rosso, No. 1:20cv954, Docket Entry 49-1, ¶¶ 130-34 (M.D.N.C. Mar. 12, 2021) (internal paragraph numbering omitted); see also id., ¶ 134 (describing "judgment for RAKIA on [Azima's hacking] counterclaim" as "procured by fraud")).

Accordingly, on March 12, 2021, see id., Docket Entry 49-1 at 1, the UK appellate court remanded Azima's hacking counterclaim for retrial before a different chancery judge, noting as it did so that "neither the parties nor the judge who hears the remitted issues will be bound by any of the findings of fact made by the [original] judge on the hacking [counter]claim," id., Docket Entry 49-1, ¶ 146. See id., Docket Entry 49-1, ¶¶ 145-46. The appellate court further noted that, on remand, "it would be necessary" for Del Rosso to testify. Id., Docket Entry 49-1, ¶ 143.

Against this backdrop, Tsiattalou avers:

In late March 2020, Mr. Oliver Moon [("Moon")], a private investigator, turned whistleblower, informed Mr. Alexander Sawyer [("Sawyer")] (who works in corporate intelligence via a company called Quaestio), that he had been instructed by a "Source A2", as he was described in the Robinson Proceeding (and who was later revealed to be a Mr. John Gunning[("Gunning")]), to make attempts to gain access to Stokoe's confidential information. These instructions continued throughout April 2020 and included hacking Stokoe's bank accounts, including its client account. It was subsequently discovered that Source A2's instructions had in turn derived from a Mr. Paul Robinson[("Robinson")], another private investigator.

(Docket Entry 4, ¶ 13.)²⁰ The Tsiattalou Declaration continues:

As he has since confirmed in an affidavit, Mr. Moon was also instructed to procure confidential information – including accessing their bank accounts – about others assisting Mr. Al Sadeq, namely, Maltin Litigation Support Group[, a legal public relations firm whose employee traveled to Dubai with Tsiattalou in March 2020 (id., ¶ 11), and Radha Stirling (at times, "Stirling") of Detained in Dubai]. The timing and coordination of this hacking demonstrates that it is designed to interfere with the Al Sadeq Litigation, and to undermine the sanctity of the confidential relationship between solicitor and client. For instance, just after the claim form and Particulars of Claim were served in the Al Sadeq Litigation and a couple of weeks before Dechert's solicitors made enquiries of Stokoe as to who was funding that litigation, Mr. Moon was instructed to obtain Stokoe's banking co-ordinates.

On April 21, 2020, Mr. Gunning was instructed to ascertain [Tsiattalou's] movements "in and out of Dubai – for Feb 2020." As mentioned above, [Tsiattalou] was in Dubai in February 2020 obtaining instructions in relation to the Al Sadeq Litigation, and became aware that [he] was the subject of surveillance and an unlawful break in.

(Id., ¶¶ 14-15 (internal paragraph numbering omitted).)

20 Sawyer had previously engaged Moon to conduct work on Stokoe's behalf, which presumably motivated Moon to disclose this situation to Sawyer. (Id.)

In Tsiattalou's view, "[t]here can be no doubt that the attempted hacking of Stokoe was motivated by, and relates to, its retainer by Mr. Al Sadeq." (Id., ¶ 16.) Tsiattalou further avers:

As mentioned above, in late March 2020, Mr. Moon informed Mr. Sawyer of Quaestio that he had been instructed to obtain confidential information from Stokoe. Mr. Moon agreed to work with Stoke [sic] and Mr. Sawyer to establish the nature and origin of the requests.

[Tsiattalou] was informed by Quaestio (and Mr. Moon has in an affidavit dated July 2, 2020 confirmed) that, pursuant to the arrangement, Mr. Moon received the following instructions from "Source A2" (an individual Stokoe eventually identified as [Gunning]):

a. On April 2, 2020, Mr Moon was instructed to obtain, amongst other things, the Stokoe's banking coordinates.

b. On April 9, 2020, Mr. Moon was instructed to access Stokoe's trading bank account and transactional data for the business bank account for the last three months. This period broadly coincides with the period that had elapsed since the issue of the Claim Form in the Al Sadeq Litigation.

c. On April 21, 2020, Mr. Moon was instructed to provide information relating to [Tsiattalou's] movements in and out of Dubai in February 2020. This period broadly coincides with the period that [Tsiattalou] attempted to visit Mr. Al Sadeq in the [UAE]. As . . . detailed above, when [Tsiattalou] visited Dubai during this time, [he] was subjected to covert surveillance.

d. On April 22, 2020, Mr. Moon was instructed to provide information relating to Stokoe's client account, including transactional information for the month of March 2020. Mr. Moon was told that it was likely information would also be sought for the period November 2019 to February 2020, a period overlapping almost exactly with the period of Mr. Al Sadeq's retainment of Stokoe.

Mr. Sawyer liaised with Stokoe to provide Mr. Moon with Stokoe's bank account documents in a format which allowed covert tracking, to identify the recipients of those documents. In this way, Quaestio established that Mr. Moon was instructed by [Gunning], who was in turn instructed by [Robinson]. Quaestio's findings are set out in a report, dated June 27, 2020, which is annexed [to the Tsiattalou Declaration ("the Quaestio Report")²¹].

Based on this information, Stokoe initiated the Robinson Proceeding in the High Court of Justice of England and Wales, Queen's Bench Division seeking, *inter alia*, to enjoin, and to obtain affidavits from, Mr. Moon, Mr. Gunning, and Mr. Robinson. . . .

Proceedings against Mr. Robinson were stayed by a consent order sealed by Justice Chamberlain, (the "Chamberlain Order"). . . . Pursuant to the Chamberlain Order, Mr. Robinson undertook to "swear an affidavit stating on oath . . . the identity of any person who has requested" that he "obtain Confidential Information from" Stokoe. Mr. Robinson swore an affidavit wherein he stated that Mr. Patrick Grayson was the source of these instructions. . . .

By letter dated November 30, 2020, Mr. Page's attorney, Stephenson Harwood, sent a letter to Stokoe with invoices for the corporate research undertaken by Company Documents Limited, Mr. Robinson's company, on behalf of Page Corporate Investigations Limited (London) and Page Group ME JLT (Dubai). One of the invoices from March 19, 2020, showed that the subject of an investigation was the Brendale Group, a group of companies associated to Mr. David Haigh who has been closely associated to Radha Stirling and who are both named in a press release attributing to their associations and linked companies. Another invoice from October 4, 2017, shows that a group of companies that were involved in RAKIA's case against Mr. Mikadze were the subject of an investigation by Mr. Robinson's company

21 As relevant here, the Quaestio Report indicates that, "in addition to requests relating to Stokoe, a number of other targets have been identified by Mr Robinson including: Maltin PR, Mr Tim Maltin and, to lesser extent, Hogan Lovells International LLP, [Azima], and [Stirling]." (Docket Entry 4-8, ¶ 3.)

as instructed by Mr. Page. The companies under investigation were all connected to Gela Mikadze who was another individual investigated by Gerrard and RAKIA in connection with Dr. Massaad.

Stokoe therefore brought further proceedings against Mr. Grayson (amongst others) by Claim Form dated July 16, 2020. . . . Those proceedings were brought, *inter alia*, to compel Mr. Grayson and Mr. Grayson's associated company, Grayson + Co Ltd, to reveal the source of their instructions, any further wrongdoing, and to obtain injunctive relief to prevent them from further wrongdoing.

The application against Mr. Grayson and Grayson + Co Ltd resulted in a consent order made by Justice Tipples, (the "Tipples Order"). . . . Pursuant to the Tipples Order, Mr. Grayson and Grayson[]+ Co Ltd undertook to "swear an affidavit stating on oath . . . the identity of any person who has requested that he "obtain Confidential Information from" Stokoe.

Mr. Grayson's affidavit (the "Grayson Affidavit") was notably brief. He stated that: "Nobody requested me to obtain Confidential Information from or pertaining to [Stokoe], directly or indirectly."

(Id., ¶¶ 33-41 (heading, citations, internal paragraph numbering, and certain parentheticals omitted) (certain ellipses and brackets in original).) The Grayson Affidavit further states that Grayson "never asked Mr Robinson to obtain Confidential Information relating to [Stokoe]." (Docket Entry 4-15, ¶ 5.)

However, approximately eight months after submitting the Grayson Affidavit, Grayson provided further information in the Grayson Proceeding that undermine the assertions in his affidavit. In particular, Grayson admitted that, on January 30, 2020, he informed "Robinson that he would be interested in any general information as to how Mr Al Sadeq was funding the Al Sadeq

[L]itigation," although he maintains that, during this conversation, he "did not ask Mr Robinson to obtain confidential information about [Stokoe]." (Docket Entry 6-3 at 3-4.) Grayson also acknowledged that, around the beginning of April 2020, he asked Robinson if "it was still possible to find out in Dubai if an individual had entered or left Dubai" and that, in response to Robinson's query whether "Grayson was interested in the travels of anyone in particular," he "mentioned Mr Tsiattalou, the senior partner of [Stokoe], as a potential person of interest" and subsequently sent Robinson an email containing Tsiattalou's identifying information. (Id. at 4.)²²

Grayson further admitted that his "interest in how Mr Al Sadeq might be funding his litigation was prompted by a general question raised with him in a telephone call on or shortly after 28 January 2020 with Mr Nicholas del Rosso of Vital Management," with whom Grayson "had a general consulting arrangement . . . (which was not contained in any written agreement) to provide general business intelligence services and advice." (Id. at 5; see also Docket Entry 6-4 (containing three-year nondisclosure agreement, dated August 30, 2018, between Vital Management and Grayson).)

22 Nevertheless, Grayson maintains that he "did not provide any instruction to Mr Robinson to investigate Mr Tsiattalou or his movements; nor did he ask Mr Robinson to obtain confidential information about [Stokoe] or to obtain information unlawfully," and he also "never asked Mr Robinson to provide information about when Mr Tsiattalou entered or left Dubai." (Id.)

Thereafter, in approximately "late March/early April 2020," Grayson and Del Rosso had another telephone conversation in which Del Rosso asked "whether it was possible to find out if someone had travelled into and out of Dubai" and, in response to Grayson's query whether "[D]el Rosso was potentially interested in the movements of anyone in particular," he "named Mr Tsiattalou and said he was the senior partner at [Stokoe]. Shortly after and as a result of that request, Mr Grayson had the conversation with Mr Robinson in or around the beginning of April 2020" described above. (Docket Entry 6-3 at 5.)

In addition, on March 22, 2021, Page disclosed in the Grayson Proceeding a letter, "dated September 16, 2020, from Allen & Overy LLP (a firm representing the Ruler and Government of [RAK]) to Stephenson Harwood LLP (the firm representing defendant Page in the Grayson Proceeding), wherein a number of statements purportedly made by defendant Page are referenced." (Docket Entry 6, ¶ 15.) As relevant here, the letter states:

1. We understand from Mr Jamie Buchanan that your client, Mr Stuart Page, has made a number of statements in communications that he had with Mr Buchanan in August and September 2020 that appear to refer to our clients, the Ruler and the Government of [RAK].

3. Our clients are concerned to understand what information your client intended to relay by his statements to Mr Buchanan. In particular, we should be grateful if your client would provide us with his explanation for the following statements:

- (a) your client referred to English High Court proceedings that have been commenced against him by Stokoe Partnership Solicitors and said: *"if I have to implicate Nick / Patrick, Decherts, Neil and the boss to get me out of this I will."* We understand that your client's reference to "the boss" is intended to be a reference to the Ruler.

Please can your client explain what information, facts or evidence your client had in mind and how he believes this implicates or otherwise relates to the Ruler.

- (c) your client said: *"what with the boss refusing to cover my costs I wish quite frankly I took the ENRC offer"*.

- (e) your client made a number of statements as to his intended future conduct including:

- (ii) *"regrettably Jamie I would have to say you know Nick and Patrick and that Nick was retained long before me and reported to at least in part to Neil.";* and
- (iii) *"I will stand my ground if I am supported I will not if I am quite frankly treated this way"*.

Please can you [sic] client confirm whether any of the above statements were intended to relate to the Ruler or the Government of [RAK]; and, if 'yes', please can your client explain what his intended actions were/are in respect of each relevant statement.

4. We note that some of your client's messages to Mr Buchanan appear to refer to our communications in respect of your client's request that our clients fund his legal costs. As we have discussed previously (e.g. in the

telephone calls between Mr Francis of our office and Mr Fordham of your office on 15 and 17 July 2020): our clients rejected your client's request and noted that the legal proceedings against your client have nothing to do with our clients; and, your client has confirmed that he has never been instructed by our clients to do any work in relation to Karam Al Sadeq, nor his lawyers, nor the proceedings that have been brought against Neil Gerrard and Dechert (amongst others).

(Docket Entry 6-6 at 2-3 (emphasis in original).)

Finally, Tsiattalou avers:

Since the issue of proceedings in the Al Sadeq Litigation, [Tsiattalou], along with others involved in the Al Sadeq Litigation, have received numerous emails and text messages which appear to be targeted attempts to access personal data. [Tsiattalou] believe[s] that these attempts amount to phishing or spear-phishing; i.e. communications which seek to trick the recipient into clicking on a link to a website which itself contains malicious software which is downloaded onto the recipient's device. Spear-phishing is a more sophisticated form of phishing where the communication contains specific information, targeted at the recipient, which makes it more likely that the recipient will click on the link.

In particular, Stirling, who has published articles about the Al Sadeq Litigation and has aided Mr. Al Sadeq in raising awareness amongst human rights activists and non-governmental organizations about his case, received a phishing email from a Google Inc. ("Google") account, dutrouxjustine@gmail.com. That same email address sent a phishing email containing Android Package files ("APK files") to Detained in Dubai. An analysis conducted of those APK files showed that the APKs communicated with a number of Ngrok server addresses. Stirling was also the subject of approximately four (4) phishing attempts using content hosted on Dropbox Inc. ("Dropbox") sent to her email address radha@radhastirling.com. Approximately twenty-six (26) phishing attempts were sent to the email addresses of [certain lawyers involved in the Al Sadeq Litigation] and Stirling from domains hosted by Cloudflare Inc. ("Cloudflare"). In addition, Google Firebase accounts were used in approximately twenty (20) phishing attempts targeting the email accounts of [those

lawyers], Stirling, and Tim Maltin, of Maltin Litigation Support Group. It is believed that these hacking attempts were perpetuated by individuals associated with the defendants in the Al Sadeq Litigation as part of an attempt to interfere with Mr. Al Sadeq's legal representation.

At approximately 5:45 a.m. on November 5, 2020, just days before a hearing in the High Court was scheduled in the Robinson and Grayson Proceedings, hackers broke into Stokoe's cloud-based IT system which the firm uses to conduct its day-to-day business. By approximately 8:45 a.m., Stokoe's IT provider was able to take measures to protect Stokoe's data and that of ten other law firms potentially affected. Consequently, Stokoe was unable to gain access to their IT system until November 9, 2020. During the time that the IT system was down, Stokoe faced significant impediments in carrying out their day-to-day business activities, including the inability to receive emails on their work addresses. Stokoe was informed by its IT provider that after evaluating the password used to orchestrate the hacking, it determined that the hacking was linked specifically to Stokoe (rather than any of the ten other law firms affected) and that Stokoe's financial material and banking data were accessed.

Stokoe has been operating since 1994. As a firm, [Stokoe] ha[s] never before 2020 been affected by such cyberattacks. [Tsiattalou] believe[s] that these various attempts to access Stokoe's confidential information are linked to its representation of Mr. Al Sadeq. Beyond the confidential information that was sought from Stokoe as described above, in Mr. Robinson's affidavit, he stated that he received the following requests for information:

- a. Information about Ms. Stirling's whereabouts, telephone numbers, and banking information; and
- b. Financial records and monthly transactional data from the bank account of Maltin PR.

Mr. Al Sadeq's Legal and Support Team has been, and remains, a target of a complicated and coordinated campaign by unknown perpetrators, within the context of their involvement in the ongoing Al Sadeq Litigation.

Accordingly, upon information and belief, Del Rosso and Vital Management have information, documents, and material which would provide evidence necessary to establish the identity of the ultimate perpetrators behind the hacking campaign targeted against Mr. Al Sadeq's [l]egal [t]eam, and in turn, aid Mr. Al Sadeq in proving the defendants' ongoing pattern of human rights abuses, their efforts to interfere with Mr. Al Sadeq's access to legal representation, and their willingness to go to extreme lengths to conceal their unlawful conduct.

(Docket Entry 4, ¶¶ 43-48 (headings and internal paragraph numbering omitted).) Thus, Applicants seek to depose Del Rosso and Vital Management. (See Docket Entries 3-1, 3-2.) In connection with those depositions, Applicants seek certain documents concerning Del Rosso's and Vital Management's interactions with CyberRoot. (See id.)

II. Ancillary American Proceedings

Separately, in December 2020, Applicants filed a Section 1782 request in the United States District Court for the Northern District of California, "seek[ing] the issuance of subpoenas directed at Google, Cloudflare, Ngrok, and Twilio SendGrid for documents and information concerning the subscriber information and IP information of accounts which were used in various phishing attempts to hack Mr. Al Sadeq's Legal and Support Team's accounts and confidential information." (Docket Entry 2 at 16 n.5.) In January 2021, the California Court directed Applicants to serve their Section 1782 application and "supporting papers on the [d]efendants in the underlying litigation, including Dechert [Defendants], and any other interested party." In re Al Sadeq, No.

3:20-mc-80224, Docket Entry 4 at 1 (N.D. Cal. Jan. 28, 2021). Dechert Defendants responded with a "Notice of Non-Opposition," which "state[s] unequivocally that they had no involvement with, or knowledge of, the purported 'online hacking campaign' that is described by the Applicant[s]. The discovery sought by the Applicant[s] is unrelated to the Dechert [Defendants] and, accordingly, the Dechert [Defendants] do not oppose the application." Id., Docket Entry 6 at 1 (emphasis omitted).

Nevertheless, in a short order with limited analysis, the California Court denied the application on the grounds that Applicants failed to establish that the requested discovery "is for use in a proceeding before a foreign tribunal," In re Al Sadeq, No. 20mc80224, 2021 WL 2828810, at *3 (N.D. Cal. Mar. 30, 2021), appeal filed, No. 21-16126 (9th Cir. July 6, 2021). In this regard, the California Court stated in full:

[Applicants] must next show that the discovery sought is for use in a proceeding before a foreign tribunal. To be "for use" in a foreign proceeding, the information sought must be relevant. *Rainsy v. Facebook, Inc.*, 311 F. Supp. 3d 1101, 1110 (N.D. Cal. 2018). Courts are permissive in construing whether discovery sought is relevant to the claims and defenses at issue in the foreign tribunal. *In re Veiga*, 746 F. Supp. 2d 8, 18-19 (D.D.C. 2010); see also *Digital Shape Techs., Inc. v. Glassdoor, Inc.*, 2016 WL 5930275, at *3 (N.D. Cal. Oct. 12, 2016) ("The party issuing the subpoena has the burden of demonstrating the relevance of the information sought."). [Applicants] describe in detail the ways in which they believe they are being surveilled and hacking attempts against them. (Dkt. 2.) [Applicants] assert that these incursions are because of their involvement in the Al Sadeq Litigation and the UK Litigation. However, [Applicants] do not establish a link between the fact

that someone might be watching or attempting to hack them and the particular claims at issue in the foreign proceedings. The Court therefore cannot find that the information sought, even if probative of hacking, would be for use in the foreign proceedings, because it is unclear how the information would be relevant to the substance of the underlying claims. [Applicants] have therefore failed to carry their burden as to this requirement.

Id.

Additionally, in October 2020, Azima sued Del Rosso and Vital Management in this Court for allegedly conspiring with, inter alia, Gerrard, Page, and Buchanan to hack Azima's computer data, including emails (the "Azima/Del Rosso Litigation"). See generally Azima, Docket Entry 1 (the "Azima Complaint"). In particular, the Azima Complaint asserts that Gerrard and Dechert hired Del Rosso and Vital Management on RAKIA's behalf to hack Azima's data, which Del Rosso and Vital Management accomplished through CyberRoot Risk Advisory Private Limited ("CyberRoot"), a company in "India that engages in illegal hacking." Id., Docket Entry 1, ¶ 2. On February 12, 2021, Azima (publically) disclosed the existence of the instant litigation to Del Rosso and Vital Management. See, e.g., id., Docket Entry 45, ¶¶ 7-13. On March 5, 2021, Del Rosso and Vital Management responded to this disclosure by stating, in the Azima/Del Rosso Litigation, the following:

On February 5, a former RAK official filed a new discovery application under 28 U.S.C. § 1782 in this District (the "Al Sadeq 1782 Application"), which, like Azima's pending discovery motion, seeks discovery from [Del Rosso and Vital Management] related to the alleged hack of Azima's data. Although the underlying foreign

proceeding does not appear to have any relation to [Vital Management], CyberRoot, or allegations of hacking, in support of that application, the petitioners there submitted a set of photographed copies of purported Kotak Mahindra Bank statements (the "Statements"). The Statements show payments from [Vital Management] to CyberRoot totaling an amount already alleged in the [Azima] Complaint.

Id., Docket Entry 47 at 4.

Despite the Application's public disclosure, no one – including Dechert Defendants, Del Rosso, Vital Management, or RAKIA – has sought to oppose the Application in the instant litigation. (See Docket Entries dated Feb. 5, 2021, to present.)

DISCUSSION

I. Section 1782

"Section 1782(a) provides that a federal district court 'may order' a person 'resid[ing]' or 'found' in the district to give testimony or produce documents 'for use in a proceeding in a foreign or international tribunal . . . upon the application of any interested person.'" Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241, 246 (2004) (brackets and ellipsis in original); see also In re Naranjo, 768 F.3d 332, 338 n.4 (4th Cir. 2014) (observing that, under Section 1782, "[a]ny 'interested person' may apply to a district court to obtain documents or testimony from another person 'for use in a proceeding in a foreign or international tribunal'"). "[Section 1782] reflects a long-term – over 150-year – policy of Congress to facilitate cooperation with foreign countries by 'provid[ing] federal-court assistance in

gathering evidence for use in foreign tribunals.'" Servotronics, Inc. v. Boeing Co., 954 F.3d 209, 212-13 (4th Cir. 2020) (brackets in original) (quoting Intel, 542 U.S. at 247).

As such, "Section 1782 affords the district courts 'wide discretion' in responding to requests for assistance in proceedings before foreign tribunals." Al Fayed v. United States, 210 F.3d 421, 424 (4th Cir. 2000). "In exercising its discretion under § 1782, the district court should be guided by the statute's twin aims of providing efficient means of assistance to participants in international litigation in our federal courts and encouraging foreign countries by example to provide similar means of assistance to our courts." Id. (internal quotation marks omitted). As the United States Court of Appeals for the Fourth Circuit has explained:

In deciding whether to grant the application and allow a subpoena to issue under the statute, the district court considers several factors identified in *Intel*[,] 542 U.S. [at] 246 This initial application process often occurs ex parte See, e.g., *In re Republic of Ecuador*, No. C-10-80225 MISC CRB (EMC), 2010 WL 3702427, at *2 (N.D.Cal. Sept. 15, 2010) (listing cases). Once the application is granted and the subpoena is issued, the subpoena target can move to quash it. *Id.*

In re Naranjo, 768 F.3d at 338 n.4.

In the referenced decision, the United States Supreme Court identified certain "factors that bear consideration in ruling on a § 1782(a) request." Intel, 542 U.S. at 264. Accordingly, once an

applicant satisfies the statutory requirements, the Court considers:

(1) whether the person from whom discovery is sought is a participant in the foreign proceedings, or instead, is a nonparty outside the foreign tribunal's jurisdiction whose evidence is presumably more dependent on the [C]ourt's assistance; (2) the nature and character of the foreign proceedings, and the receptivity of the foreign body involved to United States judicial assistance; (3) whether the application attempts to circumvent foreign proof-gathering restrictions or other policies of a foreign country or the United States; and (4) whether the requests are unduly intrusive or burdensome [and thus should be "trimmed" or rejected outright, id. at 265].

In re Peruvian Sporting Goods S.A.C., No. 18-mc-91220, 2018 WL 7047645, at *3 (D. Mass. Dec. 7, 2018) (citing Intel, 542 U.S. at 264-65).

II. Analysis

As a preliminary matter, the Court properly may proceed ex parte at this juncture, with the understanding that, if "the application is granted and the subpoena is issued, the subpoena target can move to quash it," In re Naranjo, 768 F.3d at 338 n.4; see also In re Qwest Commc'ns Int'l Inc., No. 3:08mc93, 2008 WL 2741111, at *5 (W.D.N.C. July 10, 2008) ("Issuance of the subpoena is but a first step in this process, and allows for the subpoenaed party to challenge the subpoena under Rule 45, Federal Rules of Civil Procedure, or appeal th[e magistrate judge's authorization o]rder to the district court upon a showing that its issuance was clearly erroneous or contrary to law."). Moreover, here the subpoena targets have known of the Application for an extended

period, see Azima, Docket Entry 45, ¶¶ 7-13, but have not sought to oppose the issuance of the requested subpoenas (see Docket Entries dated Feb. 5, 2021, to present). Accordingly, the Court will grant Applicants' request to proceed ex parte.

Turning to the statutory requirements, the Court first finds that Applicants qualify as "interested parties," given their status as claimants in the Foreign Proceedings. See, e.g., In re Oak Tr., No. 5:21mc7, 2021 WL 1390014, at *2 (M.D. Fla. Apr. 13, 2021) (ruling that "applicants are 'interested parties' because each expects to be a claimant in the anticipated U.K. proceeding"). The Court further finds that Applicants seek testimony and documents from an individual and entity residing in this district, as Section 1782 requires, see Intel, 542 U.S. at 246. (See Docket Entries 3-1, 3-2.) Finally, the Court finds that Applicants seek this evidence "for use" in the Foreign Proceedings.²³

As to that final statutory requirement, it bears noting that the "for use" factor imposes only a "*de minimis*" burden upon a Section 1782 applicant. In re Veiga, 746 F. Supp. 2d at 18 (collecting cases). Here, Applicants assert that "Del Rosso and Vital Management are in possession of relevant documents, materials, and information which will aid in determining the

23 The California Court's contrary determination on Applicants' request to subpoena certain technology companies does not alter that conclusion, particularly given, inter alia, the different targets and information requested.

identity of the perpetrators behind the hacking campaign targeting Mr. Al Sadeq's Legal and Support Team and lend support to Mr. Al Sadeq's claims of human rights abuses against the defendants." (Docket Entry 2 at 20.) As support for that contention, the record reflects that, on Del Rosso's own admission, Dechert hired Del Rosso and Vital Management in 2014 "to investigate assets potentially stolen from [RAK's] Government," a task that included examining "potential frauds committed by, amongst others, [Dr.] Massaad" (Docket Entry 4-4, ¶ 4), at the direction of Dechert, Gerrard, Buchanan, and other RAK governmental representatives. (See, e.g., id. at ¶¶ 4-8.)²⁴ The record further reflects that, per RAKIA's claims in the Azima Litigation, Al Sadeq participated in these alleged frauds with Dr. Massaad and Azima. (See, e.g., Docket Entry 4-2, ¶¶ 8, 168-183.) RAKIA's evidence in the Azima Litigation regarding this alleged fraud rested on Azima's confidential emails, obtained through hacking. (See, e.g., id., ¶ 384.)

RAKIA, Gerrard, and Del Rosso asserted that Page located Azima's hacked emails on the Internet, which material Gerrard then engaged Del Rosso and Vital Management to download. (See, e.g., id., ¶¶ 51-53, 336-343.11; Docket Entry 4-4, ¶¶ 5-18.) In the

24 In his trial testimony in the Azima Litigation, Del Rosso indicated that his participation in RAK's fraud investigation remained ongoing. (See Docket Entry 4-5 at 27 ("[S]ince 2014, August 2014, I've been involved somewhere in this massive investigation.").)

Azima Litigation, Del Rosso further maintained that he "did not hack Mr Azima's computers, cause him to be hacked or know who hacked him" and also "did not upload his data to the internet, cause his data to be uploaded or know who did upload his data." (Docket Entry 4-4, ¶ 20.) However, subsequently discovered evidence in the Azima Litigation indicated that Del Rosso allegedly instructed an Indian company, CyberRoot, to hack Azima's data beginning in June or July of 2015. See Azima, Docket Entry 49-1, ¶¶ 130, 132. Del Rosso responded to this evidence by admitting "that he had engaged CyberRoot to carry out work on RAKIA's behalf; and had arranged the payment to CyberRoot of the \$1 million. But he said that that was for different work which had nothing to do with Mr Azima." Id., Docket Entry 49-1, ¶ 133.

Like Azima, members of Al Sadeq's Legal and Support Team have received multiple spear-phishing and phishing emails since disclosure of their involvement in the Al Sadeq Litigation. (See, e.g., Docket Entry 4, ¶¶ 43-44; Docket Entry 4-2, ¶¶ 295-300.) Around the same time, private investigators received instructions to, inter alia, obtain these individuals' confidential information, including bank account information, and track at least some of their travel to Dubai – travel associated with the Al Sadeq Litigation. (See, e.g., Docket Entry 4, ¶¶ 14-15, 33-38, 46.) Notably, the financial information sought from Stokoe overlaps with its engagement in the Al Sadeq Litigation and addresses information

that Dechert Defendants have sought in the Al Sadeq Litigation, namely “who was funding that litigation” (id., ¶ 14). (See id., ¶ 34.) Moreover, Grayson admitted that his inquiries to Robinson regarding Tsiattalou’s travel to Dubai and the funding source for the Al Sadeq Litigation originated with Del Rosso (see Docket Entry 6-3 at 3-5), with whom Grayson had an ongoing “general consulting arrangement . . . to provide general business intelligence services and advice” (id. at 5; see also Docket Entry 6-4 (nondisclosure agreement between Vital Management and Grayson)). Page has similarly implicated Del Rosso (as well as Dechert, Gerrard, the Ruler, and Grayson) in the disputed conduct in the Grayson Proceeding. (See Docket Entry 6-6 at 2-3.)

Applicants seek production of documents related to Del Rosso’s and Vital Management’s work with CyberRoot for the period from July 1, 2015, through September 30, 2017. (Docket Entry 3-1 at 7-8; Docket Entry 3-2 at 7-8.) This time frame closely correlates to the period in which Vital Management paid CyberRoot \$1 million (see, e.g., Docket Entry 4-7 at 2-10) for either hacking Azima’s confidential information, see Azima, Docket Entry 49-1, ¶ 132, or undertaking some other efforts on RAKIA’s behalf, see id., Docket Entry 49-1, ¶ 133, during Del Rosso’s investigation into fraudulent activities allegedly involving Al Sadeq, an investigation that continued through at least the initiation of the Al Sadeq Litigation (see Docket Entry 4, ¶ 25; Docket Entry 4-5 at 27).

Applicants further seek to depose Del Rosso and Vital Management, focusing on their work with CyberRoot for “the period from January 1, 2015 to the date of [the] deposition.” (Docket Entry 3-1 at 5; Docket Entry 3-2 at 5.)

Information regarding Del Rosso’s and Vital Management’s interactions with CyberRoot during this period bears relevance to Applicants’ claims in the Foreign Proceedings. For example, the timing and method by which RAKIA obtained Azima’s confidential emails, which allegedly implicated Al Sadeq in the asserted fraud, appear relevant to Al Sadeq’s contention that RAKIA’s claims stem from political motives. Moreover, the methods employed in RAK’s “massive investigation” (Docket Entry 4-5 at 27) into Dr. Massaad, Azima, Mikadze, and Al Sadeq relate to both Al Sadeq’s claims in the Al Sadeq Litigation and to Stokoe’s Hacking Claims, particularly because Page (to whom Del Rosso, Gerrard, and RAKIA attribute the discovery of Azima’s hacked materials online) has suggested that Del Rosso, Gerrard, and the Ruler bear responsibility for at least some of the conduct at issue in the Grayson Proceeding. Further, given both the direct and circumstantial evidence linking Del Rosso and the Al Sadeq Litigation with the hacking attempts, cyberattacks, and illicit investigations regarding Stokoe and associated individuals, ascertaining whether Del Rosso and Vital Management enlisted CyberRoot to hack individuals involved in scrutinizing alleged

human rights violations by RAK and its Ruler – violations involving both Azima’s alleged co-conspirator and, as in the Azima Litigation, Dechert Defendants – qualifies as relevant to both the Al Sadeq Litigation and Grayson Proceeding. Accordingly, the Court finds that Applicants have satisfied their burden of establishing that the requested discovery satisfies the “for use” requirement of Section 1782(a).

Turning to the discretionary Intel factors, Del Rosso and Vital Managements are not parties in the Foreign Proceedings, which weighs in favor of granting Section 1782 aid. See, e.g., Intel, 542 U.S. at 264 (“[N]onparticipants in the foreign proceeding may be outside the foreign tribunal’s jurisdictional reach; hence, their evidence, available in the United States, may be unobtainable absent § 1782(a) aid.”); In re Oak Tr., 2021 WL 1390014, at *2 (granting Section 1782 request where subpoena target “will not be a party in the anticipated U.K. proceeding and, thus, [is] potentially beyond the jurisdiction of the High Court of England and Wales to compel production”). Moreover, “there is no evidence [that] the court in the United Kingdom would be unreceptive to the evidence” that Applicants seek. In re Oak Tr., 2021 WL 1390014, at *2. To the contrary, the UK appellate court has already permitted introduction of evidence regarding Del Rosso’s interactions with CyberRoot, including a new witness statement from Del Rosso, and noted the need for further testimony from Del Rosso on this issue

in the Azima Litigation. See Azima, Docket Entry 49-1, ¶¶ 130-34, 143. Similarly, no indication exists that Applicants seek the requested evidence in “an attempt to circumvent foreign proof-gathering restrictions or other policies of a foreign country or the United States,” Intel, 542 U.S. at 265. Finally, the requested discovery, which focuses on payments to CyberRoot, communications with CyberRoot, and CyberRoot’s work for Del Rosso and Vital Management (see Docket Entry 3-1 at 7-8; Docket Entry 3-2 at 7-8), appears narrowly tailored and reasonable.²⁵ As such, the discretionary Intel factors favor Section 1782 aid.

Under the circumstances, the Court will authorize the requested discovery. See Al Fayed, 210 F.3d at 424 (noting that, “[i]n exercising [their] discretion under [Section] 1782,” courts should consider Section 1782’s aims of providing effective assistance to foreign litigants and encouraging by example similar assistance from foreign courts).

CONCLUSION

Applicants have satisfied the Section 1782 statutory requirements and each of the discretionary Intel factors weighs in favor of Section 1782 relief.

²⁵ This finding “is made without prejudice to [Del Rosso and Vital Management] later contesting the requested discovery by seeking a protective order or any other relief consistent with the Federal Rules of Civil Procedure.” In re Oak Tr., 2021 WL 1390014, at *2 n.1.

IT IS THEREFORE ORDERED that the Application (Docket Entry 1) is **GRANTED**. Applicants may serve on Del Rosso and Vital Management the subpoenas attached to the Merritt Declaration as Exhibit A and Exhibit B (Docket Entries 3-1, 3-2), along with a copy of this Memorandum Opinion and the other filings in this matter (Docket Entries 1 to 6-6). In accordance with the spirit of Federal Rule of Civil Procedure 45(a)(4), Applicants shall also serve copies of the subpoenas and this Memorandum Opinion on Dechert Defendants and the defendants in the Grayson Proceeding.

IT IS FURTHER ORDERED that Del Rosso and Vital Management shall respond to the subpoenas consistent with the Federal Rules of Civil Procedure and this Court's Local Rules.

This 18th day of October, 2021.

/s/ L. Patrick Auld
L. Patrick Auld
United States Magistrate Judge